

## Department of Justice

## § 17.19

safeguarded as if it were “Confidential” information pending the determination about its classification which shall be made by the original classification authority within 30 days.

### **§ 17.15 Classification in context of related information.**

Certain information which would otherwise be unclassified may require classification when combined or associated with other classified or unclassified information, including that which the classifier knows already has been officially released into the public domain.

### **§ 17.16 Classification categories.**

(a) A determination to classify may be made only if the information concerns one or more of the categories in paragraph (b) of this section and if the unauthorized disclosure of the information reasonably could be expected to cause damage to the national security.

(b) Information must be considered for classification if it concerns:

- (1) Military plans, weapons, or operations;
- (2) The vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;
- (3) Foreign Government Information;
- (4) Intelligence activities (including special activities), sources or methods;
- (5) Foreign relations or foreign activities of the United States;
- (6) Scientific, technological, or economic matters relating to the national security;
- (7) U.S. Government programs for safeguarding nuclear materials or facilities;

(8) Cryptology;

(9) A confidential source; or

(10) Other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by the President by a person designated by the President or by the Attorney General. Requests for any such additional category of information shall be forwarded through the Department Security Officer and the Assistant Attorney General for Administration to the Attorney General for approval. Any additional categories of information approved by the Attorney

General must be reported promptly to the Director of the Information Security Oversight Office.

### **§ 17.17 Duration of classification.**

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official who has classification authority over the information. Any decision to extend an automatic declassification shall be made with respect to individual documents or categories of information. The Department is responsible for notifying holders of the information of such extensions. Any decision to extend this classification on other than a document-by-document basis shall be reported to the Department Security Officer.

(c) Information marked for declassification review under predecessor orders shall remain classified until reviewed for declassification under the provisions of this regulation.

### **§ 17.18 Classification of Foreign Government Information.**

(a) Unauthorized disclosure of Foreign Government Information or the identity of a confidential foreign source is presumed to cause damage to the national security and, accordingly, such information shall normally be assigned a classification of at least “Confidential.”

(b) If the fact that information is Foreign Government Information must be concealed, a marking shall not be used and the document shall be marked as if it were wholly of United States origin.

### **§ 17.19 Prohibitions.**

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization or agency; or to restrain competition. Information may be classified, notwithstanding that it